Command, Control, Communication, Computers and Information Technology (C4&IT)

Strategic Plan

FY13-17

Intentionally Blank

To the Men and Women of the Coast Guard:

It is my pleasure to present the U.S. Coast Guard's *Command, Control, Communications, Computers, and Information Technology (C4IT) Strategic Plan for Fiscal Years 2013-2017*. Since the initial publication of our *C4IT* Strategic Plan back in FY08, we have made major strides in improving our *C4IT* services and capabilities in support of operations throughout the Coast Guard. By continuing to build upon on this solid framework, we will provide the Coast Guard and DHS with the *C4IT* capabilities they need to save lives, safeguard our maritime borders, respond to natural and man-made disasters, interdict illegal drugs, and ensure that commerce continues to move across the high seas.

Our strategic plan is aligned and driven by Federal and Departmental guidance that mandates total IT Governance and is codified by our Commandant's guiding principles: steady the service, honor our profession, strengthen our partnerships, and respect our shipmates. This strategic plan identifies the scope and direction of Coast Guard C4IT IT governance, development and investment of our infrastructure for the next five years. By closing gaps in the five core areas listed below, the Coast Guard will continue to ensure we have the most technologically advanced C4IT services and capabilities it needs to support our enterprise in meeting mission execution.

Information: Improve, encourage and foster information sharing, quality, efficiency, and compliance with our internal and external stakeholders.

Technology: Deliver mission-focused, interoperable, and innovative solutions to enhance our C4IT capabilities for the enterprise.

Security: Enhance mission effectiveness by preventing C4IT security incidents, such as cyber attacks and intrusions, and enhancing C4IT security mitigation, user awareness, and enforcing compliance.

Governance: Govern the C4IT enterprise through the execution of Technical Authority and effective processes for enterprise architecture, capital planning and investment control, systems development, project management, performance measurement and requirements.

Organizational Excellence: Achieve organizational excellence by continually developing our C4IT workforce, collaborating with operational partners, and improving business processes by implementing best practices.

Each year we will update the CG-6 Performance Plan (Appendix A) to reflect our ongoing commitment to our C4IT strategy. By aligning our business processes to the framework listed above, we guarantee that our limited resources are being used to effectively accomplish the Coast Guard's overarching C4IT strategy for complete IT governance.

The success of this strategic plan depends on the talent, commitment and proactive involvement of each and every member of our Coast Guard community to support a Coast Guard and DHS Enterprise perspective vice narrow programmatic scope. We look forward to continuing to work with each of you; our stakeholders o achieve our mutual goals of maritime safety, security and stewardship in protecting our great Nation.

Best,

Rear Admiral Robert E. Day Jr.
Assistant Commandant for Command, Control, Communications, Computers and Information Technology
Chief Information Officer
Director, Coast Guard Cyber Command, Pre-Commissioning Detachment
United States Coast Guard

Table of Contents

INTRODUCTION

PURPOSE

The Assistant Commandant for Command, Control, Communications, Computers, and Information Technology (C4IT)/CG-6, Chief Information Officer (CIO), for the Coast Guard publishes this C4IT Strategic Plan. The purpose of this plan is to provide a unifying strategy for CG-6 to improve, integrate, and maximize the Coast Guard's C4IT capabilities in support of mission execution.

SCOPE

The intent is for members of the C4IT community and Coast Guard to use this plan to establish and prioritize recommendations for implementing improvements to the Coast Guard's C4IT infrastructure, systems, applications, products, policies, practices, and processes. The focus of this document is on activities that must occur in the next five years to begin achieving the long term goals of the Coast Guard and the Department of Homeland Security (DHS). While the goals in this plan may not be fully realized in the next five years, it is clear that coordinated activity must occur now to improve the Coast Guard's operational capabilities.

AUTHORITY

The C4IT Strategic Plan has been developed under the authority of the Assistant Commandant for C4IT, CIO, for the Coast Guard. CG-6 derives its authority for C4IT from Commandant Instruction (COMDTINST) 5401.5, Establishment of the CG-6 Directorate and Associated Duties. This COMDTINST made CG-6 the office responsible for all Coast Guard operational, business, and infrastructure C4IT assets.

At a departmental level, DHS Management Directive (MD) 0007.1, Information Technology Integration and Management, establishes the component CIO as the authority responsible for the timely delivery of Information Technology (IT) mission services. This includes the effective management and administration of all component IT resources to meet mission, departmental, and enterprise program goals.

At a Federal level, U.S. Code Title 44, Public Printing and Documents, Federal Information Policy mandates three key responsibilities for the CIO. One, the CIO must develop and maintain a strategic information resources management plan. Two, the CIO must establish goals for improving information resources' contribution to program productivity, efficiency, and effectiveness. Three, the CIO must identify methods for measuring progress towards reaching those goals. This plan addresses each of these federally mandated responsibilities.

BACKGROUND

CURRENT ENVIRONMENT

The U.S. Coast Guard, one of the nation’s five armed services, is the principal Federal agency responsible for maritime safety, security, and stewardship. As such, we protect the vital economic, environmental, and security interests of the United States. This includes the personal safety and security of the maritime public, our natural and economic resources, the global commerce infrastructure, and the integrity of our maritime borders. We are committed to addressing all threats and hazards in a manner consistent with the law and in alignment with the goals and objectives of DHS. We do this throughout the maritime domain including in U.S. ports and inland waterways, along the coasts, on the high seas, and in other regions where our maritime equities are at stake.

As a military, multi-mission, and maritime service, we have three fundamental roles: maritime safety, security, and stewardship. In each of these roles, the Coast Guard depends on C4IT to achieve its missions.

From Puerto Rico to Kodiak, in Coast Guard command centers across the United States, we optimize C4IT systems and services to capture information about suspicious activities and possible threats. By optimizing our enterprise of ships, aircraft, and small boats, we deploy C4IT assets, including sophisticated positioning and communication capabilities to keep our forces connected with our operational partners on shore, in the air, along the coasts, and on the high seas. To support the multi missions of the Coast Guard, we provide Active Duty military, reserves, civilians, and auxiliary personnel with over 700 robust C4IT products and serves to ensure they have the latest technological capabilities are available to assist them in carrying out our missions.

CHALLENGES

We operate in a continually changing and complex mission environment. As such, the way ahead poses many challenges for the Coast Guard. This is especially true in the area of C4IT as the Coast Guard becomes more dependent on technology for mission execution. As the Directorate for C4IT (CG-6), we must adapt our goals, objectives, and initiatives to fulfill the Coast Guard’s complex and continually changing mission and business needs.

The following sections outline some of the challenges that we currently face as the Coast Guard’s Directorate for C4IT.

- Balance Between Missions: After September 11, 2001, the Coast Guard’s priorities and focus shifted suddenly and dramatically. Today and into the future, as a component of DHS, the Coast Guard must dedicate more resources to homeland security missions. In addition, any unexpected event, from a man-made disaster (such as a terrorist attack) to a natural disaster (such as a hurricane), may result in a shift in resources. Further complicating this balance between missions is Coast Guard’s requirement, as a military service, to remain ready and prepared to respond to the needs of the Department of Defense (DoD). To fulfill these varied roles, we must ensure that our technology is agile and mission-focused.

- Interoperability with Partners: The Coast Guard must be able to effectively interoperate and share information across a wide range of inter- and intra-agency partners to support disaster relief, law enforcement, defense, and other mission and business areas. This demand for information sharing and interoperability is not a new issue. Previous events, such as Hurricane Katrina, prove that information sharing and interoperability can lead to mission success. Consequently, we must implement compatible equipment and standards, and define procedures and practices for information sharing to ensure seamless communications with our partners.

- Increasing Demands in an Austere Budget Environment: User expectations and requirements continually increase as technology advances. During this period of austere budgets we must effectively communicate with users to ensure that their expectations are balanced with the funding that is available to introduce enhancements to existing systems and the introduction of new technologies.

- Increasing Threats to Network and Information: From capturing intelligence about a possible threat to transmitting administrative information, we rely on our network to exchange, process, and store information 24 hours a day, 7 days a week. We must protect and defend this vital resource to assure network and information confidentiality, integrity, availability, and privacy at all times.

- Rapid Pace of Technology Advancement: Technology is progressing at an ever increasing pace. This represents a significant challenge and opportunity for the Coast Guard. As we advance, we must balance the incorporation of new technologies that improve our operational capabilities with our limited resources and funding. We must be prepared to provide innovative services to our customers by re-thinking our current C4IT approaches as technology advances.

- Rising Customer Expectations: As new technology becomes available and commonplace in the market, Coast Guard personnel continue to find new ways to leverage C4IT to perform their jobs more effectively. As technology advances, we must make informed decisions about how to deploy new capabilities to fulfill rising customer expectations.

These are but a few of the challenges that the Coast Guard must address. Our ability to select the appropriate strategies to meet these challenges will enable Coast Guard success in the future. By implementing this C4IT Strategic Plan, and the related CG-6 Performance Plan (Appendix A), we will systematically and comprehensively resolve each of these challenges.

STRATEGIC GUIDANCE

By understanding and aligning our goals to Federal, DHS, and Coast Guard strategic guidance, we can enhance Coast Guard mission execution. Figure 1 shows how Federal, DHS, and Coast Guard guidance shaped the goals, objectives, and initiatives identified later in this plan. Highlighted at the top of each box in Figure 1 are the specific guidance documents that we discuss in more detail in the following sections.

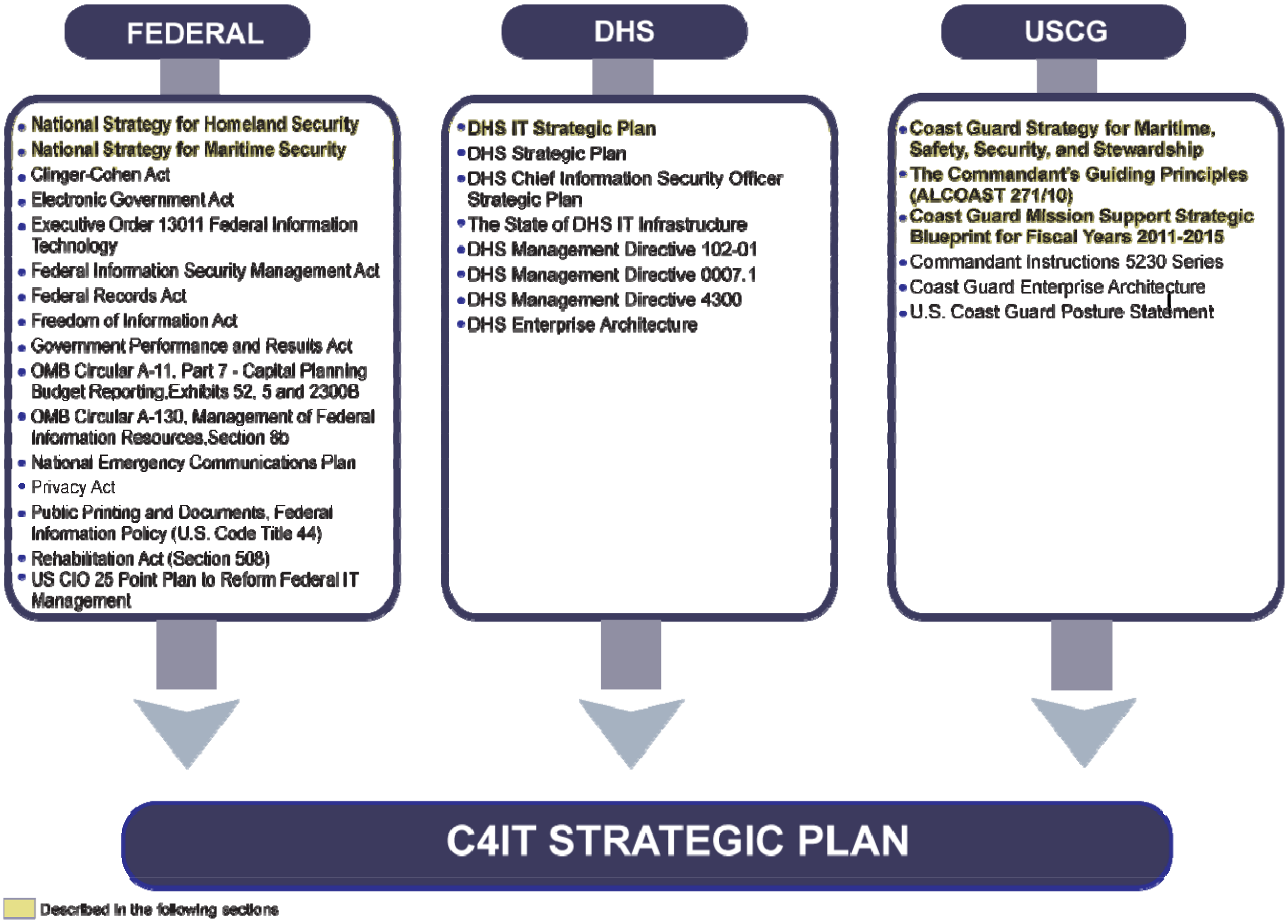
FEDERAL
National Strategy for Homeland Security
National Strategy for Maritime Security
Clinger-Cohen Act
Electronic Government Act
Executive Order 13011 Federal Information Technology
Federal Information Security Management Act
Federal Records Act
Freedom of Information Act
Government Performance and Results Act
OMB Circular A-11, Part 7 - Capital Planning Budget Reporting,Exhibits 52, 5 and 2300B
OMB Circular A-130, Management of Federal Information Resources,Section 8b
National Emergency Communications Plan
Privacy Act
Public Printing and Documents, Federal Information Policy (U.S. Code Title 44)
Rehabilitation Act (Section 508)
US CIO 25 Point Plan to Reform Federal IT Management
DHS
DHS IT Strategic Plan
DHS Strategic Plan
DHS Chief Information Security Officer Strategic Plan
The State of DHS IT Infrastructure
DHS Management Directive 102-01
DHS Management Directive 0007.1
DHS Management Directive 4300
DHS Enterprise Architecture
USCG
Coast Guard Strategy for Maritime, Safety, Security, and Stewardship
The Commandant's Guiding Principles (ALCOAST 271/10)
Coast Guard Mission Support Strategic Blueprint for Fiscal Years 2011-2015
Commandant Instructions 5230 Series
Coast Guard Enterprise Architecture
U.S. Coast Guard Posture Statement
C4IT STRATEGIC PLAN
Described in the following sections

Figure 1: C4IT Strategic Plan Guidance

Federal Guidance

The *National Strategy for Homeland Security* serves to guide, organize, and unify our Nation's homeland security efforts. It recognizes that we must continue to focus on a persistent and evolving terrorist threat while addressing the full range of potential catastrophic events that impact homeland security.

The following goals, from the *National Strategy for Homeland Security*, guide the Nation's homeland security activities:

- Prevent and disrupt terrorist attacks;
- Protect the American people, our critical infrastructure, and key resources;
- Respond to and recover from incidents that do occur; and
- Continue to strengthen the foundation to ensure our long-term success.

In addition, the *National Strategy for Maritime Security* (NSMS) serves to integrate and synchronize the existing DHS strategies for maritime security and ensure their effective and efficient implementation. The following objectives from the NSMS guide the Nation's maritime security activities:

- Prevent Terrorist Attacks and Criminal or Hostile Acts: Detect, deter, interdict, and defeat terrorist attacks, criminal acts, or hostile acts in the maritime domain, and prevent its unlawful exploitation for those purposes.

- Protect Maritime-Related Population Centers and Critical Infrastructures: Protect maritime-related population centers, critical infrastructure, key resources, transportation systems, borders, harbors, ports, and coastal approaches in the maritime domain.

- Minimize Damage and Expedite Recovery: Minimize damage and expedite recovery from attacks within the maritime domain.

- Safeguard the Ocean and Its Resources: Safeguard the ocean and its resources from unlawful exploitation and intentional critical damage.

DHS Guidance

The United States Government established DHS to secure the American homeland and protect the American people. Specifically for IT, the DHS CIO established four strategic goals for enhancing the Department's IT capabilities in support of the mission objectives in the *DHS Information Technology Strategic Plan 2011-2015*:

- Goal 1: Establish secure IT services and capabilities to protect the Homeland and enhance our Nation's preparedness, mitigation, and recovery capabilities

- Goal 2: Strengthen and unify the Department's ability to share information and services internally and with Federal, State, local, tribal, international and private industry partners.

- Goal 3: Improve transparency, accountability, and efficiencies of services and programs through effective governance and enterprise architecture.

- Goal 4: Develop and implement a comprehensive approach to IT employee recruitment, development, retention and recognition to ensure excellence in IT delivery across the Department.

The Coast Guard's C4IT goals directly align to the Department's IT goals (see Appendix B for matrices). The alignment of these two sets of goals helps to ensure that our C4IT goals and objectives fully support the Department's goals. The synchrony also provides opportunities to collaborate with the other components within DHS as they work to achieve the same goals.

U.S. Coast Guard Guidance

The Commandant's Direction

In ALCOAST 271/10 (dated May 20, 2010), Admiral Bob Papp published four guiding principles for his watch as Commandant. These principles challenge people, at every level of the chain of command, to refocus on their missions to ensure that our waterways are safe and secure. Admiral Papp's four guiding principles are as follows:

Steady the service: To reduce stress on our service and maintain the highest level of readiness we must emphasize our statutory missions, finish organizational realignment and prioritize demands for our services within the budget. We must continue to pursue replacement assets for the future. We must return to a sustainable state.

Honor our profession: At all times, we are a military organization guided by responsibility, authority and accountability. Mission excellence is our north star. Honoring our profession requires inspired leadership to develop knowledge, skills, pride and experience, in a nurturing environment, built from a foundation of clear doctrine and training.

Strengthen our partnerships: They are a force multiplier. As demand for our service continues to expand, and the threats in the maritime environment increase in complexity, a unilateral approach will not be the best or the most efficient means to achieve mission success. We can be more effective and provide greater value to our country when we forge partnerships with local, state, federal, tribal and international agencies. For the same reasons, strengthening appropriate relationships with private industry is imperative. Ultimately, strong partnerships are critical to enhancing our capability, effectiveness and credibility in the maritime domain.

Respect our shipmates: Our people are the Coast Guard's greatest asset and our ability to perform our mission ultimately depends on your health, vibrancy, training and capabilities. We must provide the best in human resource management, administrative support, wellness programs and professional development, while maintaining a safe, collaborative and productive work environment. Our service must also draw strength from the diversity of our nation.

-Admiral Bob Papp, Commandant, U.S. Coast Guard, ALCOAST 271/10

Coast Guard Strategy for Maritime Safety, Security, and Stewardship

This strategy is the framework and strategic intent that guides our activities at the Coast Guard. More specifically, it identifies the following priorities for improving the Nation's preparedness and advancing U.S. maritime interests.

- Strengthening Regimes for the U.S. Maritime Domain: The Coast Guard will work with DHS, interagency partners, U.S. maritime stakeholders, and the international community to update and strengthen existing maritime regimes and put in place new regimes where needed to address emerging challenges and threats.

- Achieving Awareness in the Maritime Domain: The Coast Guard will work with the DoD, U.S. interagency partners, state and local governments, the private sector, and the international community to implement the *National Plan to Achieve Maritime Domain Awareness* as intended by the NSMS.

- Enhancing Unity of Effort in Maritime Planning and Operations: The Coast Guard will improve its integrated planning with all partners, its network of command and control centers, and its operational capabilities. In doing this, the Coast Guard will advance unity of command where possible, and unity of effort at all times. The Coast Guard will also align its operational structure around shore based, maritime patrol, and deployable specialized forces to better allow force packaging and scalable response to all threats and all hazards. This will support the NSMS and its *Maritime Operational Threat Response Plan* (MOTR), as well as the *National Response Plan*.

- **Integrating Coast Guard Capabilities for National Defense:** The Coast Guard will better integrate its capabilities with DoD and optimize its forces within a Navy/Coast Guard relationship. This will build upon the “National Fleet” model and support the *National Maritime Strategy* (NMS) as well as the NSMS and its subordinate plans.

- **Developing a National Capacity for Maritime Transportation System Recovery:** To support the NSMS and its *Maritime Infrastructure Recovery Plan* (MIRP), the Coast Guard will leverage its authorities, responsibilities, and capabilities to lead the national planning agenda for assuring the continuity of commerce and critical maritime activities.

- **Focusing International Engagement on Maritime Governance**: The Coast Guard will focus its international efforts to assist maritime organizations and partner nations in building the sustainable regimes, awareness, and operational capabilities necessary to improve the governance of the global maritime domain.

Coast Guard’s Mission Support Strategic Blueprint

The Coast Guard’s Mission Support Strategic Blueprint for Fiscal Years 2011-2015 is driven by the Commandant’s guiding principles of Steady the Service, Honor our Profession, Strengthen our Partnerships, and Respect our Shipmates, and Deputy Commandant for Mission Support four cornerstones of Total Asset Visibility, Configuration Management, Bi-level Maintenance, and Product Line Managers. Setting an overarching vision for Coast Guard mission support, this Blueprint focuses our efforts in the following key areas:

1. **Governance**: Develop an effective governance model that integrates strategic planning with the budget process to maximize results and manage risks within current and expected resources.

2. **Organizational Integration**: Implement integrated portfolio management to support operations and lifecycle management.

3. **Common C4IT Architecture**: Establish a common command, control, communications, computers and information technology (C4IT) architecture that facilitates data driven decision making and accountability.

4. **Human Capital Alignment**: Strengthen the human capital program to provide the best workforce for Coast Guard mission execution and support.

5. **Optimal Process**: Ensure mission support core business processes deliver optimal (effective and efficient) service levels.

CG-6 MISSION & VISION

MISSION

To enhance Command, Control, Communications, Computers and Information Technology's value in the performance of CG missions by developing and aligning enterprise strategies, policies, and resource decisions with the CG Strategic Goals, mandates, and customer requirements.

VISION

A Coast Guard that is equipped with the right resources and capabilities for the right people at the right time to safeguard the Nation's Maritime domain.

CORE VALUES AND CONCEPTS

Interrelated core values and concepts guide the way we, as CG-6, conduct business. These core values and concepts are summarized below.

- C4IT Leadership: We believe that C4IT leaders must set clear technology direction, have high expectations for system delivery, create a customer-focused culture, and balance the needs of all stakeholders to ensure that we meet mission requirements. C4IT leaders must inspire their workforce and motivate them to grow professionally, contribute wholly, and be creative.

- Visibility and Transparency: We believe that all aspects of C4IT management must be visible and transparent to CG-6 system managers, as well as stakeholders, at all times during system planning, development, and support. Visibility and transparency are particularly important to C4IT spending and system performance. To this end, we support a collaborative investment management process that gives the entire organization access to C4IT priority decisions.

- Guidance: We believe in establishing guidelines that ensure organizational agility and effective acquisition, application, and management of C4IT systems through a policy and practices framework, and interactions with stakeholder organizations. Our guidelines provide an appropriate level of discipline and structure, and identify the necessary tools to deliver timely and reliable C4IT systems.

- Optimizing Outcomes: We believe in leveraging C4IT to accomplish the Coast Guard’s missions and deliver superior results. We recognize the extraordinary value of innovation when employees apply an entrepreneurial spirit by using technology as a performance enabler. With this in mind, we established the enterprise architecture (EA), systems development life cycle (SDLC), and investment management processes with maximum flexibility to ensure that technology improves Coast Guard mission and program performance.

- Partnering to Accomplish the Coast Guard Missions: We believe that no CG-6 activity can operate in isolation of Coast Guard operational missions and programs. Our success and ability to add value depends upon the ability of CG-6 to embrace, understand, and support enterprise missions and programs. As such, we must collaborate with our stakeholders to ensure that we meet requirements while following the disciplines established to govern C4IT.

CG-6 GOALS AND OBJECTIVES

OVERVIEW

The following strategy consists of the goals and objectives that CG-6 plans to accomplish over the next five years. By achieving these goals and objectives, we will realize the Commandant's strategic vision of the future. The goals are purposely broad with the objectives and initiatives focused primarily on a five-year timeframe. Building on the objectives, the CG-6 Performance Plan (Appendix A) identifies specific initiatives that will enable us to achieve the broader goals. Initiatives will be refined as we progress within objectives. As shown in Figure 2, the goals align to five central themes: technology and innovation, security, efficient information delivery, governance, and organizational excellence.

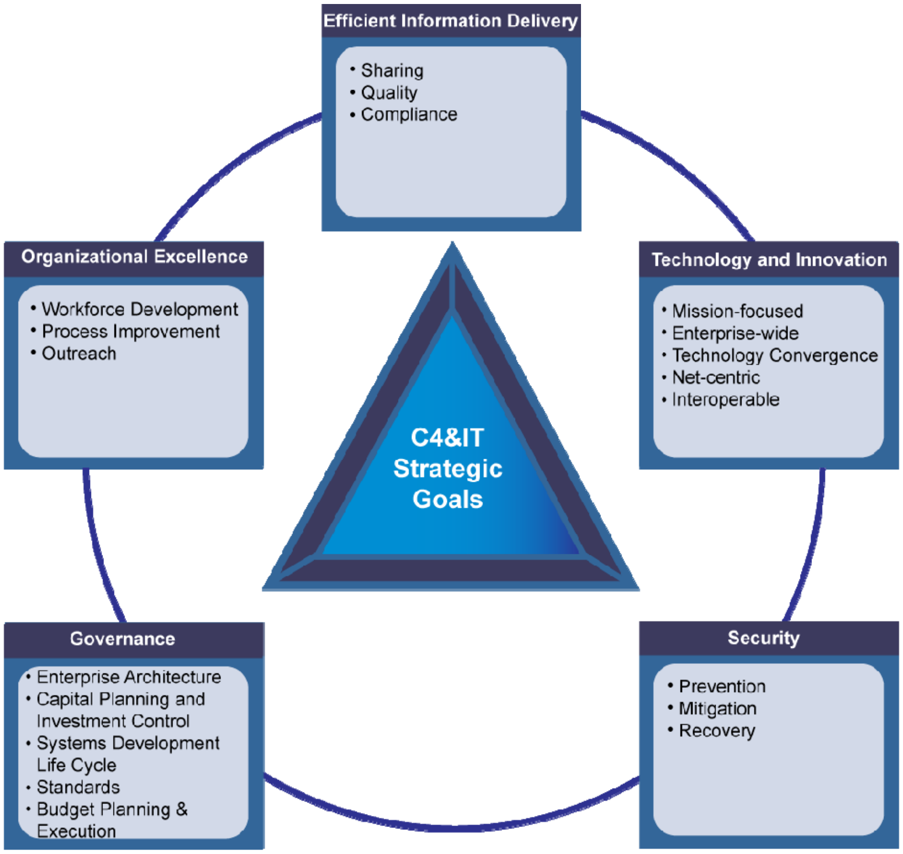

Figure 2: CG-6 Goals Overview

GOAL 1: EFFICIENT INFORMATION DELIVERY

Improve and encourage information sharing, quality, and compliance with internal and external partners.

Intent

Coast Guard mission execution, tactical maneuvers, and command and control depend on our ability to share current and valid information. As such, our personnel must be able to manage the information required to perform their duties and make better decisions. This includes, but is not limited to, tactical, surveillance, law enforcement, financial, and readiness data. In addition, as the Coast Guard becomes more dependent on information sharing, it is increasingly important for us to be able protect information quality and enhance information efficiency. We must also ensure compliance with departmental guidance regarding the protection, transmission, and management of information. This includes the adoption of DHS Enterprise Data Management Office (EDMO) practices in support of the DHS Information Sharing Environment. By doing so, we can help to improve mission execution and performance results.

Objectives

1.1 Sharing: Enable information sharing by ensuring that information is visible, understandable, accessible, and interoperable throughout the Coast Guard and with external partners.

1.2 Quality: Promote information quality by establishing processes and procedures to make sure that the Coast Guard's information is valid, consistent, and comprehensive.

1.3 Compliance: Achieve the intent of Federal and departmental information management legislation and policies, including compliance with privacy, Freedom Of Information Act (FOIA), and records management guidance.

GOAL 2: TECHONOLOGY AND INNOVATION

Deliver mission-focused, interoperable, and innovative C4IT solutions for the enterprise.

Intent

Coast Guard missions are increasingly dependent on the quality of our technology. Operators and support staff use C4IT solutions throughout the Coast Guard to safeguard our oceans and waterways, enforce maritime laws, and serve our Nation. Interoperable and net-centric solutions allow our operators to communicate seamlessly with internal and external partners such as Federal agencies (including the DoD and its components); state, local, and tribal governments; and intelligence agencies. In addition, during times of war, our ability to transition from governmental responsibilities to defensive capabilities requires optimized and innovative C4IT resources. To satisfy mission demands and operator needs, we must deliver mission-focused and interoperable C4IT using enterprise-wide and net-centric solutions, an optimized infrastructure, and wireless communications.

Objectives

2.1 Mission-focused: Satisfy operator C4IT requirements by delivering mission-focused solutions that improve mission execution and business processes, leverage enterprise solutions, and adhere to the Coast Guard Enterprise Architecture (CGEA).

2.2 Enterprise-wide: Define, implement, and enforce standards for supportable and enterprise-wide C4IT systems, applications, products, and standards to enable interoperability, seamless communications, and consolidation.

2.3 Technology Convergence: Optimize the Coast Guard C4IT environment and reduce costs of operation by consolidating and integrating infrastructure in alignment with the Department’s IT modernization and transition strategy.

2.4 Net-Centric: Leverage network technologies to discover and exchange needed information in a timely manner.

2.5 Interoperable: Identify and replace stove-piped networks, systems, and applications with C4IT solutions that are interoperable within the Coast Guard and with our partners.

GOAL 3: SECURITY

Enhance mission effectiveness by preventing C4IT security incidents, such as Cyber attacks and intrusions, and enhancing C4IT security mitigation and recovery.

Intent

As the Coast Guard becomes more dependent on networked communications to accomplish its mission, it is increasingly important to protect the integrity of the network and the information it stores and transmits. As such, any interruption, delay, or degradation in C4IT capabilities can prevent access to critical information and processes. To protect our vital C4IT resources, the Coast Guard must follow best practices, found within industry and Government, to create a layered defense for the systems that the Coast Guard relies on for mission execution. Additionally, we must develop appropriate policies, acquire and field equipment, monitor our networks, train our workforce, and remain vigilant in our efforts to protect and maintain the integrity of the Coast Guard's computer and communication networks. By preventing C4IT security issues and enhancing C4IT security mitigation and recovery, we can support international stability and national defense.

Objectives

3.1 Prevention: Enhance C4IT security by ensuring that proper safeguards and archiving processes are in place to ensure the confidentiality, integrity, availability, and privacy of information and compliance with legal requirements.

3.2 Mitigation: Improve the Coast Guard's ability to detect and respond to C4IT security incidents in a timely manner with minimal disruption to systems and the Coast Guard's ability to carry out its missions.

3.3 Recovery: Enhance Continuity of Operations Planning (COOP) to respond effectively to security-related threats and natural disasters, and rapidly restore Coast Guard systems and data.

GOAL 4: GOVERNANCE

Govern the C4IT enterprise through the execution of technical authority and effective processes for enterprise architecture, capital planning and investment control, systems development, standards and budget planning and execution.

Intent

The fundamental purpose of executing C4IT governance activities within the Coast Guard is to enable the strategic and tactical alignment of C4IT budgets, investments, projects, and system development with the Coast Guard's priorities and goals. Using our technical authority we will maximize return on investment, mitigate risk, and ensure business and technical alignment to the CGEA. Effective governance will improve the Coast Guard's ability to meet the cost, schedule, and performance parameters of its C4IT investments.

Objectives

4.1 Enterprise Architecture: Implement an accurate, current, and complete CGEA as the single source of C4IT business and technology information throughout the Coast Guard to improve decision-making.

4.2 Capital Planning and Investment Control: Establish effective policies and processes to govern the development and deployment of C4IT throughout the Coast Guard and ensure effective oversight and financial management, and compliance with laws, regulations, and policies.

4.3 Systems Development Life Cycle: Facilitate the SDLC process to ensure the collection, validation, and fulfillment of requirements; adherence to the CGEA; and the design and support of comprehensive solutions.

4.4 Standards: Influence the development of international and industry standards.

4.5 Budget Planning and Execution: Establish effective policies and processes to govern the planning efforts for the CG-6 Budget and ensure proper execution of funds.

GOAL 5: ORGANIZATIONAL EXCELLENCE

Achieve C4IT organizational excellence by continually developing our workforce, collaborating with internal and external partners, and improving business processes.

Intent

The Coast Guard depends on its people to perform its mission. Creating an environment that fosters organizational excellence begins with equipping, developing, and preparing our people for personal, professional, and organizational success. We can do this by providing them with the correct education, training, and professional experience needed to achieve C4IT competencies. In addition, we must communicate the value of C4IT and the CG-6 mission, vision, and strategy to enable our people to meet organizational goals. Organizational excellence also requires that processes are continually improved and streamlined to provide efficient and convenient access to C4IT resources. Mission execution is the ultimate goal of organizational excellence.

Objectives

5.1 Workforce Development: Equip our people for personal, professional, and organizational success so that we may achieve our mission with a workforce that is trained, prepared, safe, and diverse.

5.2 Process Improvement: Establish, institutionalize, and continually update processes to ensure streamlined, integrated, and optimized use of C4IT resources.

5.3 Outreach: Communicate the value of C4IT, and the CG-6 mission, vision, and strategy.

THE WAY AHEAD

This strategic plan establishes the goals and objectives for CG-6, and demonstrates how they align with the overall Coast Guard and DHS strategic plans. Supporting this strategy, Appendix A: FY13 CG-6 Performance Plan, identifies specific initiatives, milestones, and critical success factors needed to progress toward achieving these goals and objectives.

In essence, the CG-6 Performance Plan is the tactical plan for CG-6. It describes the initiatives that we are executing in support of CG-6 goals. All of the work we do as CG-6 should support one or more of our strategic goals and objectives. As such, all of our major deliverables should fall within the scope of at least one of the initiatives described in the CG-6 Performance Plan. This alignment with the CG-6 strategic goals ensures that we are using our limited resources to satisfy our strategic goals.

We update both the C4IT Strategic Plan and the CG-6 Performance Plan on a yearly basis. The strategic plan contains high-level goals and objectives while the performance plan contains initiatives that we will complete to achieve our goals and objectives. We split multi-year initiatives into milestones to reflect how an initiative will progress over the next five years. More detail is provided for the current fiscal year than for upcoming fiscal years. This ensures that the plan contains sufficient detail to accurately track progress throughout the year.

Our success with completing the milestones documented in this plan will be included as part of an overall CG-6 “dashboard.” We will describe the status of each milestone as “red,” “yellow,” or “green.” Each status will depend on the progress that we are making toward successfully completing the initiative. Green milestones are milestones that were completed on time. Yellow milestones are ones that were completed late or are at risk of being met. Red milestones are milestones from the current fiscal year that were not completed. We will automatically record all incomplete items at the end of the year as “red.”

Together the C4IT Strategic Plan and the CG-6 Performance Plan will provide our CG-6 community with clear direction on our goals and objectives, and a snapshot of our progress toward achieving these goals. Communicating this information to all of CG-6 will help us join together to provide the best possible service to our customers and better align our resources to support the Coast Guard’s mission.

APPENDIX A: FY13 CG-6 PERFORMANCE PLAN

Full document available for download on CGPortal:
https://collab.uscg.mil/dm/atom/library/3b4ea2004dd98a4a9828d9e6d02d3bcd/document/107038804d75f7c49e92df2a4d041897/media?errorPage=true&resolve=false

Table of Contents

2.4 Objective: Net-Centric

2.4.1 SIPRNET Modernization

2.5 Objective: Interoperable

2.5.1 Coast Guard Electronic Chart Display and Information System (CG ECDIS) Development

2.5.2 Ultra High Frequency (UHF) Military Satellite Communications (MILSATCOM) Integrated Waveform (IW) Transition

2.5.3 Very High Frequency (VHF)/Ultra High Frequency (UHF) Land & Maritime Mobile Radio Infrastructure

3 Goal: SECURITY

3.1 Objective: Prevention

3.1.1 Over The Air Rekeying (OTAR)

3.1.2 Personally Identifiable Information (PII) Training

3.1.3 Privacy Compliance/Privacy Threshold Analyses (PTAs)

3.1.4 Strengthening Information Security throughout the Coast Guard

3.1.5 OSC Conversion to DoD Server Hardening Guidelines

3.1.6 Build and maintain a prioritized list of IT Critical Infrastructure and Key Resources (CIKR)

3.1.7 Build Information Assurance Program

3.1.8 CG Auxiliary Secure and Universal System Access

3.1.9 CG Auxiliary Secure Information Exchange

3.2 Objective: Mitigation

3.2.1 Computer Network Defense (CND) Capabilities

3.3 Objective: Recovery

3.3.1 Mobile Command Center (MCC) Development

3.3.2 Contingency SATCOM

4 GOAL: GOVERNANCE

4.1 Objective: Enterprise Architecture

4.1.1 Coast Guard Enterprise and Segment Architecture

4.1.2 Coast Guard Enterprise Architecture Board (EAB) and Related EA Reviews

4.1.3 Enterprise Architecture (EA) Tools

4.2 Objective: Capital Planning and Investment Control

4.2.1 Governance Process Integration

4.2.2 CG-9 Alignment

4.2.3 Information Technology Acquisition Review (ITAR) Process

4.2.4 Section 508 Program Management

4.2.5 Acquisition Processes Communication and Workflow

4.2.6 OMB CPIC Requirements

4.3 Objective: Systems Development Life Cycle

4.3.1 Manage the Systems Development Life Cycle (SDLC)

4.3.2 COMDTINST M10550, Electronics Manual, Update

4.3.3 Telephony Systems Policy

4.4 Objective: Standards

4.4.1 Strengthen Spectrum Program to Ensure Mission Success

4.4.2 Modernization of International Treaty and National Regulations

4.5 Objective: Budget Planning and Execution

4.5.1 CG-6 Budget Formulation

4.5.2 CG-6 Budget Execution

4.5.3 Legislative Processes

4.5.4 Audit Management

4.5.5 Internal Controls Marked for Deletion

5 GOAL: ORGANIZATIONAL EXCELLENCE

5.1 Objective: Workforce Development

5.1.1 C4IT Professional Development

5.1.2 IT/Program Manager Certification Policy

5.2 Objective: Process Improvement

5.2.1 Enterprise Project/Portfolio Management ePM

5.2.2 NTNO Program

5.2.3 Configuration Management Oversight of NTNO and C4I

5.2.4 C4IT Strategic Plan Adherence

5.2.5 Transition to Efficient Sustainment of Deepwater Command, Control, Communications, Combat, Computing, Intelligence, Surveillance, and Reconnaissance (C5ISR) Systems

5.3 Objective: Outreach

5.3.1 Communication of the CG-6 Strategy and Related Strategic Activities

APPENDIX B: STRATEGIC ALIGNMENT MATRICES

Alignment of DHS IT Goals and Coast Guard C4IT Goals

USCG C4IT GOALS DHS CIO GOALS	Information	Technology	Security	Governance	Organizational Excellence
Goal 1: Establish secure IT services and capabilities to protect the Homeland and enhance our Nation’s preparedness, mitigation and recovery capabilities.		✓	✓		
Goal 2: Strengthen and unify the Department’s ability to share information and services internally and with Federal, State, local, tribal, international and private industry partners.	✓	✓			
Goal 3: Improve transparency, accountability, and efficiencies of services and programs through effective governance.				✓	
Goal 4: Develop and implement a comprehensive approach to IT employee recruitment, development, retention and recognition to ensure excellence in IT delivery across the Department.					✓

Source: DHS Information Technology Strategic Plan Fiscal Years 2011-2015

Alignment of the Coast Guard Strategy for Safety, Security and Stewardship and C4IT Goals

USCG C4IT GOALS USCG STRATEGY FOR SAFETY, SECURITY & STEWARDSHIP	Information	Technology	Security	Governance	Organizational Excellence
Strengthen regimes for the U.S. maritime domain			✓	✓	
Achieve awareness in the Maritime Domain	✓	✓	✓	✓	
Enhance unity of effort in maritime planning and operations	✓	✓	✓	✓	✓
Integrate Coast Guard capabilities for national defense	✓	✓	✓	✓	
Develop a national capacity for Marine Transportation System recovery	✓	✓	✓	✓	
Focus international engagement on improving maritime governance	✓	✓	✓	✓	

Source: U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship (2007)

Alignment of the CG-DCMS Business Plan and Coast Guard C4IT Goals

USCG C4IT GOALS CG-DCMS OBJECTIVES	Information	Technology	Security	Governance	Organizational Excellence
Governance	✓	✓	✓	✓	✓
Organizational Integration				✓	✓
Common C4IT Architecture	✓	✓	✓	✓	
Human Capital Alignment					✓
Optimal Process	✓	✓	✓	✓	✓

Source: Coast Guard’s Mission Support Strategic Blueprint for Fiscal Years 2011-2015

1. Governance: Develop an effective governance model that integrates strategic planning with the budget process to maximize results and manage risks within current and expected resources.

2. Organizational Integration: Implement integrated portfolio management to support operations and lifecycle management.

3. Common C4IT Architecture: Establish a common command, control, communications, computers and information technology (C4IT) architecture that facilitates data driven decision making and accountability.

4. Human Capital Alignment: Strengthen the human capital program to provide the best workforce for Coast Guard mission execution and support.

5. Optimal Process: Ensure mission support core business processes deliver optimal (effective and efficient) service levels.

APPENDIX C: ACRONYMS

AAP(s)	Advanced Acquisition Plan(s)
ADEX	Active Directory Exchange
AES	Advanced Encryption Standard
AIS	Automatic Identification System
ALD	Aviation Logistics Division
ALS	Automated LORAN System
AMHS	Automated Message Handling System
AMVER	Automated Mutual-assistance Vessel Rescue system
APO	Asset Project Office
AOA	Analysis of Alternatives
ATO	Authority to Operate
BCWP	Budgeted Cost of Work Performed
BCWS	Budgeted Cost of Work Scheduled
BOD	Business Operations Division
BSD	Base Support Services Division
C&A	Certification and Accreditation
C2	Command and Control
C21	Command 21
C3CEN	Command and Control Engineering Center
C4	Command, Control, Communications, and Computers
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
C4IT	Command, Control, Communications, Computers, and Information Technology
CAC	Common Access Card
CAMSLANT	Communications Area Master Station Atlantic
CAMSPAC	Communications Area Master Station Pacific
CAO	Chief Acquisition Officer
CAS	Core Accounting System
CDRP	Contingency and Disaster Recovery Plan
CFO	Chief Financial Officer
CG	Coast Guard
CG-DCMS	Coast Guard’s Deputy Commandant of Mission Support
CG ECINS	Coast Guard Electronic Charting Integrated Navigation System
CG OneNet	Coast Guard OneNet
CG Portal	Coast Guard Portal
CG-LIMS	Coast Guard Logistics Information Management System
CGA	Coast Guard Academy
CGAP	Coast Guard Acquisition Process
CGBI	Coast Guard Business Intelligence
CGDN+	Coast Guard Data Network
CGEA	Coast Guard Enterprise Architecture
CGMS	Coast Guard Messaging System
CGONe	Coast Guard One Network
CIAO(s)	Commandant’s Intent Action Order
CIM	Commandant Instruction Manual
CIO	Chief Information Officer
CIRC	Computer Incident Response Center
CMMi	Capability Maturity Model Integration
CMS	Content Management System
CND	Computer Network Defense
COBIT	Control Objectives for Information and related Technology
COE	Center of Excellence

COMDTINST	Commandant Instruction
CONOPS	Concept of Operations
COOP	Continuity of Operations Planning
COP	Common Operating Picture
CPIC	Capital Planning and Investment Control
CPU	Central Processing Unit
CRRT	CIAO Reorganization Review Team
CUI	Controlled Unclassified Information
DAA	Designated Accreditation Authority
DAC	Data Asset Catalog
DCMS	Deputy Commandant for Mission Support
DES	Data Encryption Standard
DGPS	Differential Global Positioning System
DHS	Department of Homeland Security
DIACAP	Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMS	Defense Messaging System
DoD	Department of Defense
DOG	Deployable Operations Group
DOJ	Department of Justice
DOORS	Dynamic Object Oriented Requirements System
DRS	Disaster Recovery System
DSES	Directory Services and Exchange Services
EA	Enterprise Architecture
EAB	Enterprise Architecture Board
EACOE	Enterprise Architecture Center of Excellence
EADS	Enterprise AIS Data Service
EAM	Enterprise Asset Management
EC	Engineering Change
eCG	Electronic Coast Guard
EDC	Enterprise Data Catalog
EDMO	Enterprise Data Management Office
EGMO	Enterprise Geospatial Management Office
eMICP	enhanced Mobile Incident Command Centers
ESB	Enterprise Service Bus
ESD	Engineering Services Division
ESU(s)	Engineering Support Unit(s)
EVM	Earned Value Management
EXSTAGE	Execution Stage
FDCC	Federal Desktop Core Configuration
FEMA	Federal Emergency Management Agency
FINCEN	Finance Center
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FORCECOM	Force Readiness Command
FSAM	Federal Segment Architecture Methodology
FY	Fiscal Year
GCCS	Global Command and Control System
GDC4S	General Dynamics C4 Systems
GFE	Government Furnished Equipment
GIS	Geographic Information System
GMT	Generally Mandated Training
GOCO	Government Owned, Contractor Operated

GPS	Global Positioning System
HAS	Historical Archive System
HF ALE	High Frequency Automatic Link Establishment
HR	Human Resources
HRMS	Human Resources Management System
HSPD	Homeland Security Presidential Directive
IDP(s)	Individual Development Plans
IA	Information Assurance
ICGS	Integrated Coast Guard Systems
IG	Inspector General
INCONUS	Intercontinental United States
IOC	Initial Operational Capability
IOC	Interagency Operation Center
IP	Internet Protocol
IPv6	Internet Protocol Version 6
IRB	Investment Review Board
ISC(s)	Integrated Support Command(s)
IT	Information Technology
ITAR	Information Technology Acquisition Review
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunications Unit
IW	Integrated Waveform
KMF	Key Management Facility
LAN	Local Area Network
LCMO	Life Cycle Management Organization
LIMS	Logistics Information Management System
LoB	Line of Business
LORAN	Long Range Aids to Navigation
LORSTA(s)	LORAN Station(s)
LRIP	Low Rate Initial Production
MAP	Mission Action Plan
MCC	Mobile Command Center
MCV	Mobile Communications Vans
MD	Management Directive
MDA	Maritime Domain Awareness
MIEM	Maritime Information Exchange Model
MILSATCOM	Military Satellite Communications
MIPR	Military Interdepartmental Purchase Request
MIRP	Maritime Infrastructure Recovery Plan
MISLE	Maritime Information for Safety and Law Enforcement
MLC(s)	Maintenance and Logistics Command(s)
MMSI(s)	Maritime Mobile Service Incident(s)
MPLS	Multi-protocol Label Switching
MOE	Measures of Effectiveness
MOTR	Maritime Operational Threat Response Plan
MOA(s)	Memorandum of Agreement(s)
MOTR	Maritime Operational Threat Response
MOU(s)	Memorandum of Understanding(s)
MS EA	Microsoft Enterprise Agreement
MSAM	Major Systems Acquisition Manual
MT&E	Maritime Test and Evaluation
NAIS	Nationwide Automated Identification System
NARA	National Archives and Records Administration
NIEM	National Information Exchange Model

NIPRNET	Unclassified but Sensitive Internet Protocol Router Network (formerly called the Non-Classified Internet Protocol Router Network)
NIST	National Institute of Standards and Technology
NLECC	National Law Enforcement Communications Center
NMS	National Maritime Strategy
NOC	Network Operations Center
NSPD	National Security Presidential Directive
NSMS	National Strategy on for Maritime Security
OAP	Ocean Action Plan
OAS	Organizational Assessment Survey
OCIO	Office of the Chief Information Officer
OFCO	Operating Facility Change Order
OGAs	Other Government Agencies
OIG	Office of the Inspector General
OMB	Office of Management and Budget
ORD	Operational Requirements Document
OSC	Operations Systems Center
OTAR	Over-the-air-rekeying
OUTCONUS	Outside the Continental United States
PBX	Private Branch Exchange
PEP	Policy Enforcement Point
PHS	Public Health Service
PIA(s)	Privacy Impact Assessment(s)
PII	Personally Identifiable Information
PFD	Personnel and Facilities Division
PM	Project Management
PMBoK	Project Management Book of Knowledge
PMO	Project Management Office
PNT	Position Navigation and Timing
PO&AM	Plan of Action and Milestones
POC	Point of Contact
PORD	Preliminary Operational Requirements Document
PPRB	Policy and Practice Review Board
PSB	Products and Standards Board
PTA	Privacy Threshold Analysis
PTAs	Privacy Threshold Analyses
Q1,2,3,4	Quarter one, two, three, four
R&D	Research and Development
RAP	Resource Allocation Plan
RAS	Remote Access Service
RCC	Remote Control Console
RDC	Research and Development Center
RF	Radio Frequency
RFP	Request For Proposal
RSS	Real Simple Syndication
SAP	Stand-Alone Proxy
SATCOM	Satellite Communications
SBU	Sensitive But Unclassified
SDA	Systems Development Agent
SDLC	Systems Development Life Cycle
SELC	Systems Engineering Life Cycle
SETAB	Systems Engineering Technical Advisory Board
SFLC	Surface Forces Logistics Center
SIPRNET	Secure Internet protocol Router Network
SOA	Service Oriented Architecture
SOC	Security Operations Center
SOR	System of Record

SORN(s)	System of Record Notice(s)
SPAWAR	Space and Naval Warfare Systems Command
SRCUS	Short-Range Communications Upgrade System
SSA	System Support Agent
TASC	Transformation and Systems Consolidation
TCM	Telecommunications Manual
TCTO	Time Compliant Technical Order
TEAMS	The Enterprise Architecture Management System
TIC(s)	Trusted Internet Connection(s)
TISCOM	Telecommunication & Information Systems Command
TSA	Transportation Security Administration
TTP	Tactics, Techniques, and Procedures
UHF	Ultra High Frequency
USCG	United States Coast Guard
USCGC	United States Coast Guard Cutter
VHF	Very High Frequency
WAGB	Polar Class Icebreaker
WAN	Wide Area Network
WBS	Work Breakdown Structure
WHEC	Coast Guard High Endurance Cutter
WLB	Seagoing Buoy Tender
WLI	Coast Guard Buoy Tender, Inland
WLIC	Inland Construction Tenders
WLM	Coast Guard Buoy Tender, Coastal
WLR	River Buoy Tender
WMEC	Coast Guard Medium Endurance Cutter
WMSL	National Security Cutter
WPB	Coast Guard Patrol Boat
WPC	Patrol Coastal
WTGB	Coast Guard Icebreaking Tug
WYTL	Small Harbor Tug
XML	eXtensible Markup Language

APPENDIX D: DEFINITIONS

Command, Control, Communications Computers, and Information Technology

Command, Control, Communications, Computers, and Information Technology (C4IT) consists of any equipment or interconnected system or subsystem of equipment, or technique used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of digital, voice, or video data or information to the appropriate levels of command. This includes command and control networks, common operational picture systems, information assurance services, communication products and standards, computers, ancillary equipment, software, firmware, procedures, services (including support services), and related resources.

Enterprise Architecture

Enterprise Architecture (EA) is the discipline that synthesizes key business and technology information across the organization to support better decision-making. EA provides useful and usable information products and governance services to the end-user while developing and maintaining the current and target (to-be) architectures and transition plan for the organization. The information in the EA, includes: results of operations, business functions and activities, information requirements, supporting applications and technologies, and security.

Measure of Effectiveness

A measure of effectiveness (MOE) is a criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect.

Service Oriented Architecture

Service Oriented Architecture (SOA) is a computer systems architectural style for creating and using business processes, packaged as services, throughout their lifecycle. SOA also defines and provisions the IT infrastructure to allow different applications to exchange data and participate in business processes. These functions are loosely coupled with the operating systems and programming languages underlying the applications. SOA separates functions into distinct units (services), which can be distributed over a network and can be combined and reused to create business applications. These services communicate with each other by passing data from one service to another, or by coordinating an activity between two or more services. SOA concepts are often seen as built upon and evolving from older concepts of distributed computing and modular programming.

Systems Development Life Cycle

The SDLC is a sequence of seven phases used to produce, operate, and support C4IT systems. These phases begin with the identification of need and span all facets of a C4IT system's life cycle, including planning, acquisition, deployment, operation, and retirement of a system. The SDLC Practice is based on industry and government best practices and shall be kept current through updates to the SDLC Practices. SDLC Practices shall be promulgated separately and shall identify inputs, outputs, procedures, and products for each phase. For more information about the Coast Guard's SDLC process, see COMDTINST 5230.66.

APPENDIX E: REFERENCES

Department of Defense (2007). *Joint Publication 1-02, "DoD Dictionary of Military and Associated Terms"*. As amended through 17 October 2007. Retrieved 20 March 2008, from http://www.dtic.mil/doctrine/jel/doddict/

Department of Homeland Security (2004). *Securing Our Homeland, U.S. Department of Homeland Security Strategic Plan.*

Department of Homeland Security (2011). *Office of the Chief Information Officer, Information Technology Strategic Plan: Fiscal Years 2011-2015.*

Executive Office of the President (2005). *The National Strategy for Maritime Security*. Retrieved 21 May 2008, from http://www.whitehouse.gov/homeland/maritime-security.html#intro.

Executive Office of the President (2007). *The National Strategy for Homeland Security*. Retrieved 21 May 2008, from http://www.whitehouse.gov/homeland/maritime-security.html#intro.

Kurzweil, Ray (2001). *Essay: The Law of Accelerating Returns.* Retrieved 30 March 2008, from http://www.kurzweilai.net/meme/frame.html?main=/articles/art0134.html.

U.S. Coast Guard. *Commandant's Intent Action Orders*.

U.S. Coast Guard (2007). *The U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship*.

U.S. Coast Guard (2008). *The U.S. Coast Guard Enterprise Architecture Executive Handbook*. Retrieved 15 May 2008, from http://cgea.uscg.mil/

US Coast Guard (2011) *Coast Guard's Mission Support Strategic Blueprint for Fiscal Years 2011-2015*.

APPENDIX F: DOCUMENT CHANGES

Change Order	**Date**
Publication of FY10-14 version	01/06/2010
C4IT SC initiatives in the Performance Plan update	06/17/2010
Publication of the FY11-15 version	02/15/2011
Publication of the FY13-17 version	11/20/2012

ASSISTANT COMMANDANT C4&IT

CG-6